TABLE OF CONTENT
STANDARD GUIDELINES ON THE IMPLEMENTATION OF ANTI MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM FOR COMMERCIAL BANKS

PREFACE

One of obligations that must be complied by the Bank upon the enactment of Bank Indonesia Regulation Number 11/28/PBI/2009 dated on July 1, 2009 concerning Implementation of Anti Money Laundering and Combating the Financing of Terrorism Program (AML and CFT Program) for Commercial Banks shall be development of a guideline on implementation of AML and CFT Program. By considering some adjustments conducted on such regulation previously thru PBI No.3/10/PBI/2001 dated on June 18, 2001 as latter amended with PBI No.5/21/PBI/2003 dated on October 17, 2003 concerning Application of Know Your Customer Principle that refers to international standards, in which 40 + 9 Financial Action Task Force on Money Laundering (FATF) Recommendations, as the supporting effort to prevent crimes of money laundering and the financing of terrorism, a guideline is deemed necessary as its implementation.

By realizing such demand, Bank Indonesia together with representatives of Banks have established a task force that is responsible to develop the Standard Guidelines on the Implementation of AML and CFT Program for Commercial Banks hereinafter referred to as Standard Guideliens. In developing such Guidelines, a Task Force shall also consider international best practices on AML and CFT Program applied in other countries. In addition, development of such Guidelines also considers some inputs provided by representatives of Banks and other sources. As of development of such Standard Guidelines, it is expected that Banks may develop a Guideline on the Implementation of AML and CFT Program that complies with minimum requiremetns determined in provisions concerning the Implementation of AML and CFT Program.

Jakarta, 30 November 2009

CHAPTER I
INTRODUCTION

Financial institutions, especially banks, are vulnerable being likely used as media for committing crimes of money laundering and/or the financing of terrorism because they offer many options of transactions that can be utilized by launderers and/or terrorists' funders in order to commit their crimes. Thru various options of transactions available in which among others is money remittance, the bank is a gateway whereby proceeds of crimes or terrorists' finance enter into the financial system and then those may be benefited for the interest of criminals. For example, launders may withraw back such money to be used as if those are legitimate and can no longer be detected its origins. At the same time, perpetrators of the financing of terrorism can use such money for financing terrorist activity.

A. Definition, Stages and Modus of Operandi of Money Laundering

1. Money Laundering or internationally known as *money laundering* shall be an act of placing, transferring, disbursing, spending, donating, contributing, entrusting taking out of the country, exchanging, or other such acts related to, assets known or reasonable suspected by a Person to constitute proceeds of crime, for the purpose of concealing or disguising the origins of assets as if such assets shall be legitimate.
2. In principal, money laundering process can be classified into 3 (three) stages as the following :
    a. **Placement** shal be an act of placing cash derived from a crime into financial system, or an act of placing demand deposits (checks, bank drafts, time deposits, and others) back into financial system, in particular banking system.
    b. **Layering**, shall be an act of transferring assets derived from a crime (dirty money) that have been successfully placed into a Financial Services Provider (especially a bank) as the result of placement to other

Financial Services Providers. For example, performing multiple transactions or wire transfers.

c. **Integration**, shall be an act of using assets derived from a crime that have been successfully entered into financial system thru placing or layering as if such assets are legitimate (clean money) for financing legal business activities or refinancing their criminal activities. For example, purchasing assets and commencing/conducting business activities.

3. Some money laundering modus operandi that are commonly used by launderers are as the following:

a. **Smurfing** shall be an act of preventing reporting obligation by dividing transactions engaged by various doers.

b. **Structuring** shall be an act of preventing reporting obligation by dividing transactions into smaller amount transactions.

c. **U Turn** shall be an act of disguising the origins of proceeds of crime by turning back transactions in which later those proceeds are sent back into its origin account.

d. **Cuckoo Smurfing** shall be an act of disguising the origins of sources of fund by tranferring funds derived from their criminal activity using third party's account that is waiting for incoming wire transfer from overseas or unwittingly acknowldeged by third party concerned that funds recieved shall be "proceeds of crime".

e. **Purchasing luxury assets/goods** shall be hiding the ownership status of luxury assets/goods including transferring assets without being detected by financial system.

f. **Goods exchange (barter)** shall be preventing to use cash or other finacial instruments so that those cannot be detected by financial system.

g. **Underground Banking/Alternative Remittance Services** shall be an act of sending money thru informal mechanism performed on the ground of trust.

h. **Utilization of third party** shall be transactions engaged by using identity of third party with the purpose to prevent that identity of actual party who is true owner of proceeds of crime is not being detected.

i. **Mingling** shall be merging proceeds of crime with proceeds of legitimate business activity in order to disguise the origins of such funds.

j. **Utilization of false identity** shall be transactions engaged using false identity as an effort in complicating detection of identity as well as location of money launderers.

B. Financing of Terrorism

1. The financing of terrorism shall be utilization of assets for terrorists' activity either directly or indirectly. The financing of terrorim is principally different type of crime than money laundering but both have similarity, which is using financial services as media for committing a crime.
2. Money laundering crime has an objective to disguise the origins of assets, while the financing of terrorism is aimed to support terorists' activity either by providing assets that are proceeds of crime or assets derived lawfully.
3. In preventing banks being used as media for committing the financing of terrorism, banks must implement AML and CFT Program sufficiently.

C. Reporting to the Center for the Reporting and Analysis of Financial Transactions (PPATK)

Bank shall oblige to submit reports on Suspicious Financial Transaction or Suspicious Transaction Report (STR) and Cash Transaction Report (CTR) to the Center for the Reporting and Analysis of Financial Transactions (PPATK) based on provisions of Law concerning Money Laundering Crime. Procedures for reporting both STR and CTR shall refer to guidelines issued by PPATK.

D. Policies on the Implementation of Anti Money Laundering and Combating the Financing of Terrorism Program (AML and CFT Program)

1. AML and CFT Program shall be program that must be implemented by banks in engaging a business relationship with Customers or Walk In Customers. Such program shall include matters required under 40 + 9 Financial Action Task Force (FATF) Recommendations dan the Basel Committee on Banking

Supervision as the efforts to prevent Banks from being used as media or targets for committing crimes both directly and indirectly by criminals.

2. Customer Due Diligence (CDD) shall be one of principal instruments within AML and CFT Program. CDD shall not only be essential in the support of eradication of crimes of money laundering and the financing of terrorism, but also for implementing prudential banking principles. Implementation of CDD shall assist to protect banks from risks occurred in banking business activity such as operational, legal and reputation risks as well as to prevent banking industry being used as media or targets for committing crimes, especially money laundering and the financing of terrorism.
3. As an effort in minimizing utilization of Banks as media for committing crimes of money laundering or the financing of terrorism, Banks are required to implement AML and CFT Program. Such Program shall be part of implementation of Bank Risk Management and at least shall include as the following:
    a. active supervision of the Board of Directors and the Board of Commissioners*;*
    b. policies and procedures;
    c. internal control;
    d. information management system; and
    e. human resources and training.
4. In implementing AML and CFT Program, the Bank is required to have in place written policies and procedures that cover at least the following:
    a. request of information and documents*;*
    b. Beneficial Owner;
    c. document verifications;
    d. simplified CDD;
    e. termination of a businessa relationship and refusal of a transaction;
    f. high risk areas and Political Exposed Persons (PEP);
    g. CDD implementation procedure performed by a third party;
    h. updating and monitoring;
    i. Cross Border Correspondent Banking;
    j. wire transfer; and

k. record keeping and reporting.

5. Policies and procedures above shall be developed into Guidelines on the Implementation of AML and CFT Program and must consider information technology factor that is potentially being misused by perpetrators of money laundering or the financing of terrorism including when the Bank launches new products or services. In implementing Guidelines on the Implementation of AML and CFT Program effectively, such guidelines must be communicated to all staff and enforced consistently and continuously.

CHAPTER II
MANAGEMENT

In the support of implementation of AML and CFT Program, besides requiring an awareness from the Board of Directors and the Board of Commisioners, the Bank shall oblige to establish a Special Unit or appoint the Bank's officer who is responsible on the implementation of AML and CFT Program. An active role of the Board of Directors and the Board of Commissioners is deemed necessary in developing effectiveness of implementation of AML and CFT Program since the role of the Board of Directors and the Board of Commissioners will influence the organizational objectives achivement rating in implementing AML and CFT Program. In addition, the role of the Board of Directors and the Board of Commissioners may also motivate employees and operational units in promoting the establishment of compliance culture within all levels of an organization. The creation of well-built corporate governance within an organization will support supervision over enforcement of Guidelines of the Implementation of AML and CFT Program developed.

1. Active Supervision of the Board of Directors or the Board of Commissioners

a. Active Supervision by the Board of Directors of a Bank

Active supervision by the Board of Directors of a Bank shall cover at least as the following:

1) Ensuring the Bank shall have policies and procedures on AML and CFT Program;
2) Recommending written policies and procedures on AML and CFT Program to the Board of Commisioners;
3) Ensuring that implementation of AML and CFT Program is performed based on written policies and procedures determined;
4) Ensuring that an operational unit performing policies and procedures on AML and CFT Program is separated from an operational unit assigned to monitor its implementation;

5) Establishing a Special Unit that enforces AML and CFT Program and/or appointing an officer duly responsible on implementation of AML and CFT Program at the Head Office;
6) Ensuring that an appointed officer who is responsible on implementation of AML and CFT Program shall have sufficient capability and authority in accessing all information on Customers and other relevant information;
7) Conducting supervision over compliance of operational units in enforcing AML and CFT Program;
8) Ensuring that branch offices and assisting-branch offices of the Bank possess employees assigned to carry out functions of a Special Unit or an officer duly responsible on implementation of AML and CFT Program;
9) Ensuring that written policies and procedure on AML and CFT Program are in line with changes and developments of products, services and technology of the Bank as well as the development of modus of money laundering or the financing of terrorism;
10) Ensuring that all employees, especially from relevant operational units and new employees, have participated in periodical training in relation with AML and CFT Program;
11) Holding a commitment on implementation of AML and CFT Program such as by providing sufficient resources; and
12) Understanding, identifying and minimizing risks that might be occurred in implementing AML and CFT Program, for example operational risk, legal risk, concentration risk and reputational risk.

b. Authority and Duty of the Board of Directors

1) Authority and duty of the Board of Directors shall cover at least as the following :
    a) Developing policies and strategies of written and comprehensive Risk Based Approach (RBA);
    b) Being duly responsible on implementation of policies of RBA and risks exposure taken by the Bank completely;
    c) Determining and evaluating transactions that require an approval from the management officer; and

d) Conducting periodical evaluation in order to assure the accuracy of policies, procedures and determination of risk rating from high risk areas, Politically Exposed Person (PEP), Cross Border Correspondent Banking.

2) In implementing policies on RBA, the Bank shall oblige to perform:

a) Processes of risks identification, measurement, monitoring and controlling against all risk factors that are substantial minimum by conducting an analysis on:

(1) Risks' chateristics attached at the Bank; and

(2) Risks from high rigks areas, PEP, Cross Border Correspondent Banking.

b) In implementing risk measurement, the Bank shall oblige at least to perform :

(1) Periodical evaluation; and

(2) Improvement of measurement system of risk rating.

c. Roles and Duty of the Compliance Director

In implementing an active supervision of the Board Directors, the Compliance Director shall have power and duty at least:

1) To determine actions required to assure the Bank has met provisions of Bank Indonesia concerning AML and CFT Program and other relevant laws and regulations;

2) To assure that scopes of an active supervision of the Board of Directors have been met sufficiently;

3) To monitor and maintain compliance of the Bank on all commitments developed by the Bank to Bank Indonesia such as commitments prescribed in an Action Plan, Work Plan on Data Updating, and results of Bank Indonesia Examination in relation with implementation of AML and CFT Program;

4) To monitor performance of a Special Unit and/or the Bank's officer duly responsible on implementation of AML and CFT Program;

5) To provide recommendations to the Principal Director regarding an officer who will chair a Special Unit or duly responsible on implementation of AML and CFT Program;

6) To provide an approval on STRs; and

7) To propose an Action Plan and Work Plan on Data Updating prior being submitted to Bank Indonesia.

d. Active Supervision of the Board of Commisioners

An Active Supervision of the Board of Commissioners shall cover at least as the following:

1) To provide an approval against policies on AML and CFT Program;

2) To monitor performance of the Board of Directors in implementing AML and CFT Program including commitments developed by the Bank to Bank Indonesia; and

3) To monitor compliance of the Board of Directors in implementing AML and CFT Program thru the Compliance Director and/or Internal Audit Unit of the Bank.

2. A Special Unit

a. The Establishment of A Special Unit

1) The Special Unit is deemed necessary to be established if in implementing AML and CFT Program, the Bank requires an operational unit that specially carries out such Program.

2) In the event based on considerations of operational burdens and complexity of business activity that the Bank may not comply with the requirements on the establishment of a Special Unit, the Bank shall oblige at least to appoint the Bank's Official authorized in implementing AML and CFT Program.

3) Such position may be held two posts by the Bank's Official who has other duty with a condition that the operational unit implementing policies and procedures on AML and CFT Program is disintegrated with the operational unit that supervises its implementation so that holding two posts is allowed insofar such other duty is not part of the operational like the risk management operational unit.

b. Organizational Structure

1) In implementing its duty, a Special Unit shall report and be responsible to the Compliance Director.

2) If the Bank has not established a Special Unit yet and only appointed the Bank's official, particularly on implementation of AML and CFT Program, the official concerned shall report and be responsible to the Compliance Director.

3) All operational units of the Bank shall oblige to implement AML and CFT Program under coordination of a Special Unit of the Head Office of such Bank. This considers that operational units that interact directly with Customers are the front gate that prevent the Bank from money laundering and the financing of terrorism.

4) The operational units must assure that internal control operates properly, timely and effectively as well as must make sure that all employees of operational units have entitled sufficient training program.

5) In order that directions and provisions given by s Special Unit can be implemented acceptably, the Bank shall oblige to possess sufficient operational mechanism documented by any relevant operational unit to be reported to the Official of a Special Unit or the officer duly responsible on implementation of AML and CFT Program. Such operational mechanism shall also consider anti tipping off and information secrecy.

c. Power and Duty of A Special Unit

Main duty of a Special Unit or the Bank's officer duly responsible on the implementation of AML and CFT Program shall be:

1) To monitor the availability of system for supporting AML and CFT Program;

2) To monitor updating of Customers' profiles and Customers' transactions profiles;

3) To conduct coordination and monitoring on the implementation of policies on AML and CFT Program with relevant operational units that interact with Customers;

4) To assure that policies and procedures are in line with the development of current AML and CFT Program, banking products' risks, business activity and complexity of the Bank and volume of the Bank's transactions;

5) To obtain a potential financial transaction report (red flag) from relevant operational units that interact with Customers and to perform an analysis on such report as well;
6) To identify a transaction that meets with criteria on suspicious;
7) To prepare an STR and other reports as stipulated under Law concerning Money Laundering Crime to be submitted to PPATK upon an approval from the Compliance Director;
8) To monitor that:
   a) There exist a sufficient operational mechanism from any relevant operational unit to a Special Unit or an officer duly responsible on implementation of AML and CFT Program by maintaining information secrecy;
   b) Relevant operational units shall perform function and duty in order to prepare reports on potential Suspicious Financial Transaction prior being submitted to a Special Unit or the officer duly responsible on implementation of AML and CFT Program; and
   c) High risk areas associated with AML and CFT exist by referring to prevailing provisions and sufficient information sources.
9) To monitor, analyze and recommend training requirements on AML and CFT Program for employees of the Bank; and
10) To take part as a contact person to authorized agencies (such as Bank Indonesia, PPATK, and Law Enforcement Agency) in relation with implementation of AML and CFT Program.

d. Requirements of A Special Unit's Officer or an Officer duly responsible on Implementation of AML and CFT Program at the Head Office

The Bank's officer duly responsible in enforcing AML and CFT Program shall oblige to meet requirements as follow:

1) To have sufficient knowledge on AML and CFT and other regulations related with banking financing and products;
2) To have authority to get an access on all information regarding Customers and other relevant information in order to perform his/her duty; and
3) To have sufficient experiences in banking.

e. Employees who Perform Functions of A Special Unit or Implement AML and CFT Program at the Head Office

1) Any branch office of the Bank is required to possess an employee who performs part of functions of a Special Unit or implements AML and CFT Program. For branch offices of the Foreign Exhance Bank, this provision shall also be applicable to an Assisting Branch Offices.
2) An employee performing functions of a Special Unit concerned shall not be an employee of the operational units. However, in a case that the Bank is impossible to have an employee from non operational unit to perform such functions, Branch Offices of the Bank and Assisting Branch Offices of the Foreign Exchance Bank may assign an employee from the operational unit for performing functions of a Special Unit.
3) Power and duty of an employee who performs functions of a Special Unit as referred to in number 2 above shall be as the following:
    a) To assure that policies, procedures and other relevant regulations on implementation of AML and CFT Program have been enforced effectively.
    b) To monitor and review any validity of processes, an examiner's checklist and supporting documents when opening an account.
    c) To assure that an approval of acceptance and/or refusal of a request for opening an account or transaction by a prospetive customer or walk in customer (WIC) categorized as high risk shall be provided by the management officer within relevant operational unit or site Branch Office.
    d) To coordinate and monitor customers' data updating process and to assure that such data updating has been reported to Bank Indonesia.
    e) To obtain suspicious financial transaction reports from relevant operational units and to conduct an analysis on such reports to be submitted to a Special Unit at the Head Office.
    f) To provide inputs related with implementation of AML and CFT Program to employees of relevant operational units or Branch Offices as required.

g) To monitor, analyze and recommend training requirements on AML and CFT Program to employees at relevant operational units or Branch Offices to a Special Unit at the Head Office.

CHAPTER III
CDD AND EDD POLICIES

Costumer Due Dilligence (CDD) shall be activities in the form of identification, verification, and monitoring performed by Banks to ensure that transactions correspond to Customer's profiles. In the case that the Bank engages a business relationship with a high risk Customer with respect to the probability of money laundering and terrorism financing, the Bank shall oblige to conduct a more comprehensive CDD procedure named as Enhanced Due Diligence (EDD).

1. Banks are required to implement CDD procedure when:
    a. Engaging a business relationship with prospective Customers. In the case that an account is a joint account than CDD is performed against all account holders of such joint account;
    b. Engaging business relationship with customer not holding an account at the Bank. In this case including the Customer from other Banks where the Bank unable to access the information of that Customer (Walk In Customer (WIC)). Example: A is a Customer of the branch office of foreign Bank "X" in Singapore and wants to engage a transaction with the branch office of a foreign Bank "X" in Indonesia. A is not holding an account at the branch office of foreign Bank "X" in Indonesia and foreign Bank "X" unable to access the profile information of A which provided in the system of the branch office of foreign Bank "X" in Singapore. When engaging a transaction at the branch office of foreign Bank "X" in Indonesia, A is categorized as WIC. In the case that the branch office of foreign Bank "X" in Indonesia able to access the profile information of A which provided in the system of the branch office of foreign Bank "X" in Singapore, A is categorized as a Customer.
    c. the Bank has doubts about the veracity or adequacy of accuracy of previously obtained Customer, parties receiving power of attorneys, and/or beneficial owner identification data;
    d. There is a suspicious transaction related with money laundering and/or terrorist financing.

2. Banks shall perform CDD against Existing Customer and Existing Recipient Banks and or Intermediary Banks using Risk Based Approach if:

Customer Excluding Recipient Bank /Intermediary Bank	Recipient Bank /Intermediary Bank
a. there is significant increase in the values of a transaction	there are substantial modifications on the profiles of a Recipient Bank and/or Intermediary Bank
b. there is significant modification on a customer's profile	available information on profiles of a Recipient Bank and/or Intermediary Bank have yet to be supported with information as referred to in Article 31 paragraph (1) PBI No. 11/28/PBI/2009 concerning on Implementation of AML and CFT Program
c. information of a customer's profiles described in the Customer Identification File is not furnished with documents as referred to in Table 2, Table 3, and Table 4 on Chapter V	
d. using anonymous or fictitious accounts	

3. In the event the prospective Customers/Customers/WIC meet the following provisions:
   a. classified as high risk or PEP;
   b. utilize high risk banking products to facilitate money laundering or financing of terrorism;
   c. perform transactions with high risk countries; or
   d. perform transactions inconsistent with its risk profiles,

Banks shall perform EDD agasint the prospective Customers/Customers/WIC concerned. If the result of EDD gives a clear underlying, the monitoring against such transaction shall be conducted normally, however, if a clear underlying unable to search out, the Bank shall perform a stricter monitoring against such transaction.

CHAPTER IV
CUSTOMERS CLASSIFICATION USING RISK BASED APPROACH

A. Customers' Classification

1. In the support of implemention of effective policies and procedures on CDD, the Bank requires to implement risk based approach.
2. In implementing the Customers' acceptance, the Bank shall oblige to classify Customers based on risks' rate on potential commissions of money laundering or the financing of terrorism.
3. Customers' risk rates shall consist of low, medium and high.
    a. If the Customer has low risk rate then the Customer concerned may be subject an exemption of some requirements.
    b. If the Customer has medium risk rate then the Customer concerned may be subject requirements as determined by prevailing provisions.
    c. If the Customer has high risk rate then the Customer concerned shall be subject procedures on Enhanced Due Dilligence.
4. Customers classification must be documented and monitored continuingly.
5. Sufficient risk assessment is necessary to be implemented on the Customers who have entered into business relationship within certain period of time by considering the Customers' information and profiles as well as needs of the Customers on products and services offered by the Bank.
6. Monitoring shall be performed in order to assure conformity of risks' rates determined.
7. If there is inaccuracy between the Customers' transctions/profiles and risks' rates determined, the Bank shall oblige to adjust risks' rates thru the following means:
    a. To apply CDD procedure for the Customers who are initially categorized as low risk to be medium risk based on determination of new risks' rating.

b. To apply EDD procedure for the Customers who are initially categorized as low or medium risk to be high risk or PEPs.

B. Determination of Risks' Profiles Using Risk Based Approach

1. Risk profile shall describe risk rate of the Customers, products and services that have potential money laundering or the financing of terrorism.
2. The Bank shall oblige to have procedures of risk based approach in according with level of business compexity of the Bank and are managed sufficiently.
3. Risk profile shall be final score of all assessment's components determined based on the most dominant rating of all components. Risk profile classification shall contain of low, medium and high risks.
4. If the most dominant rating does not exist nevertheless balancing or similar composition of assessment's components exists, risk profile used shall be the most severe risk profile.
5. Determination of risk rating shall be inapplicable for the Customers categorized as PEPs. Thus, if there is a prospective Customer or the Customer due to his/her occupation or position is classified as PEP, the Customer concerned shall be automatically classified as high risk.
6. Determination of risk profile shall be implemented thru an analysis on the following issues:
   a. The Customer's Identity

      For example, a condition of the Customer's identity that needs to be analyzed shall be as the following:

      1) The Customer does not have the identification document but has a statement letter issued by the competent authority informing that a person concerned:
         a) Is a local citizen and has the address as mentioned in information provided to the Bank; and/or
         b) Has resided within long periods of time.
      2) Data/information on the Customer's identiy has been inaccurate.

3) Duration of the Customer's identification document has been expired but there is no modification on the address of the Customer concerned in which this has been confirmed by the Bank.
4) The identification document of the prospective Customer is false or the identification document is original but data/information described is fictitious.
5) The supporting documents of the prospective Customer, especially documents on a legal person, are incomplete, for example a business license, Article of Assosiation, the Authorized Parties who act to represent a company.

b. Business location

For example, business location of the Customer that needs to be analyzed shall be as the following:

1) Business location of the prospective Customer is in a Jurisdiction classified as high risk country by an international agency or organization on conditions of such jurisdiction.
2) Business location of the Customer is in the territory whose criminal rate is high on smuggling or illegal products.
3) Business location of the Customer is in free trade zone.
4) Companies that are located in countries or territories classified as tax haven.

c. The Customer's Profile

For example, conditions of the Customer's profiles that need to be analyzed shall be as the following:

1) The Customer who does not have regular incomes.
2) The Customer categorized as PEP or has a relationship with PEP.
3) A government officer, especially related with public services.
4) Law enforcement agency.
5) Persons who carry out types of activity or business sectors that are vulnerable with money laundering.
6) Parties mentioned in the United Nations list or other list published by an international organization on terorists, terrorist organizations

or organizations that finance or collect funds for terrorists activities.

d. Volume of transactions

For example, conditions of volume of transaction that needs to be analyzed shall be as the following:

1) When opening an account, the Customer engages a transaction whose value is large or significant but information on sources of fund and purposes of such transaction are improper with the profiles or the purpose of an account opening.
2) The Customer engages multiple transactions in small amounts of money but collectively shall be large or significant transactions.
3) Cash transactions in large amount of money.

e. The Customer's Business Activity

For example, conditions of the Customer's business activity that needs to be analyzed shall be as the following:

1) Business activity that provides money exchange services;
2) Business activity that provides money remittance services;
3) Cash based business activity such as grocery stores, parking management, restaurants, gas stations, phone minutes traders;
4) Business activity that provides legal documentation services;
5) Business activity that sells real estate, stocks, jewelries, automobiles or other assets;
6) Business activity that markets its products thru internet;
7) Export/import trading company;
8) Advocates, accountants or financial consultants; or
9) Multi level marketing business activity.

f. Ownership structure for the Customer of a legal person

For example, conditions of the Customer of a legal person that needs to be analyzed shall be as the following:

1) A legal person's ownership structure is complex so that an access of information is limited;
2) Composition of a legal person's owners is dominated by foreign persons;

3) There is the beneficial owner who controls a company;
4) There is negative news in mass media on the beneficial owner of such company so that risk rate of a company is high; or
5) A company established and/or owned by a legal person applies legal system in tax haven countries (whereby information on ownership of Ultimate Beneficial Owner is difficult to get) or if the ownership of such company is based on bearer shares (so that modification of shareholders are easily carried out).

g. Other information:

Location of a domicile: persons who reside and/or have funds derived from countries that have applied FATF Recommendations insufficiently.

7. Besides matters as mentioned in point 6, the Bank may develop itself methodology in getting risk profiles of the Customers based on the needs and risk profiles of each Bank.

An example of risk profiles classification matrix:

	Low	Medium	High
The Customer's Identity	- Submit more than one applicable identities	- Data/information of identity of the prospective Customer is expired, but the Customer remains being cooperative to conduct updating	- Data/information of identity of the prospective Customer is false or origin but fictitious, for example, an ID card is not issued by the competent authority, inaccurate data, etc. - data / information of identity is insuitable with domicile or the Customer always moves from one place to another or may not be reached (such as phone

	Low	Medium	High
			numbers) - when opening an account, the Customer used his/her address whose territory is outside territory of Indonesia
Business Location	- business location that is nearby the Bank or acknowledged by the Bank	- business location is distant from the Bank's location	- business location of the Customer is under free trade zones
The Customer's Profiles	- Farmers	- An employee of a Company	- Classified as PEP. - Meet criteria determined by PPATK (besides PEP) - Employees of a company categorized as high risk such as shell company
Volume of Transaction	- Volume of transaction is low, for example less than Rp 5,000,000 (five million Rupiah)	- The increase of volume of transaction is insufficient or significant but it is supported with sufficient documents or still considered reasonable	- Transaksi tunai dalam jumlah besar

	Low	Medium	High
Business Activity	- Vegetables traders at traditional markets	- Foreign exchange houses or mone remittance services	- Cash based business activity such as grocery stores, parking management, restaurants, gas stations, phone minutes traders - Utilization of L/C for export and import that is not originated from or forwarded to territory of Indonesia - Mutual fund traders
Ownership structure	- does not have the controller and composition of shareholders is available in public data	- Information on shareholders are unavailable in public data	- A company whose shareholders are nominee
Other information	- No other negative information	- Has other business besides an employee of a company	- The Customer has a loan facility whose collateral is on behalf of other person's name (either cash / goods) that has not firm relationship - The Customer who provides the power of attorney to other party for conducting

	Low	Medium	High
			withdrawals from the Customer's account as from a request for appoint an account is approved.

CHAPTER V
PROCEDURES OF ACCEPTANCE, IDENTIFICATION AND VERIFICATION (CUSTOMER DUE DILLIGENCE)

A. Policies on the Acceptance and Identification of the Customer

1. The Bank shall oblige to possess policies on the acceptance of a Customer and Identification of a prospective Customer as well as in relation with WIC that cover at least as follows:
    a. Risk based approach application by classifying Customers based on risk rating on potential monay laundering or the financing of terrorism.
    b. The request of information on propective Customers as follows:
        1) Identify of a prospective Customer;
        2) Identity of Beneficial Owner if a Customer is representing the Beneficial Owner;
        3) Sources of fund;
        4) Average income;
        5) The purpose and intended nature of the business relationship or transactions that will be engeged by a prospective Customer with the Bank; and
        6) Other information that makes the Bank be able to identify the profiles of a prospective Customer.
    c. The request of evidence of identity and supporting documents from a prospective Customer.
    d. Examination on the accuracy of identity and supporting documents presented by a prospective Customer.
    e. The request of other identity card issued by the competent authority if there is an unlikelihood on existing identity card presented.
    f. The Bank may intervew a prospective Customer if required in order to obtain certainty on the accuraty of information, identification documents and the supporting documents of a prospective Customer.

g. Prohibition to open or maintain an anonymous account or the account using a fictitious name.

h. Conducting face to face communication with a prospective Customer when commencing to enter into a business relationship in order to ensure the accuracy of identity of a prospective Customer.

i. An awareness on transactions or business relationship with a prospective Customer come from or related with countries that have applied FATF Recommendaitons unsufficiently.

j. Completion of verification process against a prospective Customer prior entering into a business relationship with a prospective Customer.

k. Refusing the opening of an account of a prospective Customer and or refusing to pursue a transaction engaged by WIC who meets the following criteria:

1) Does not comply with provisions or requirements as stipulated in Articles 11, 13, 14, 15, 16, 17, 18 and 19 of Bank Indonesia Regulation Number 11/28/PBI/2009 concerning Implementation of Anti Money Laundering and Combating the Financing of Terrorism Program;

2) Is known to use improper identity and or presenting irregular information; or

3) Is formed as Shell Banks or with the Bank that allows his/her accounts are used by Shell Banks.

l. Keeping records of a prospective Customer or WIC who meet criteria mentioned above into a seperate list and reporting a person concerned as an STR if his/her transaction is unusual or suspicious.

2. Policies and procedures of the acceptance of Customers shall also be applicable to Customers who do not possess an account at the Bank (WIC).

B. The Request of Information

1. Prior entering into a business relationship with the Customer, the Bank shall oblige to request for information that makes the Bank be able to identify the profiles of a prospective Customer.

2. The prospective Customers must be identified and classified into natural persons and legal persons. If the prospective Customer is a legal person then the classification of legal persons concerned shall also cover the Beneficial Owner.
3. Information that must be requested from the prospective Customer who has been classified shall cover at least as follows:

Table 1: Information on the Prospetive Customers

Natural Person		Legal Person (including Bank)	Charity/ Association	State/Government Institutions, international organization, foreign country representatives
a.	Full name including alias.	Name of company	Name of Charity/Association	Name
b.	Number of the Identification Document	Business license number issued by the competent authority	Business/type of activity license number (including business/type of activity) of the purpose of a foundation or registration number issued by the competent authoirty	Domicile
c.	Address described in the identification document	Domicile	Domicile	
d.	Current domicile including phone number if any	Place and date of establishment	Place and date of establishment	
e.	Place and date of birth	Type of legal entity	Type of legal entity (if it is formed as a legal entity)	

Natural Person		Legal Person (including Bank)	Charity/ Association	State/Government Institutions, international organization, foreign country representatives
f.	Nationality	The Identity of Beneficial Owner if any	The Identity of Beneficial Owner if any	
g.	Sources of fund	Sources of fund	Sources of fund	
h.	Gender	The purpose and intended nature of the business relationship	The purpose and intended nature of the business relationship	
i.	Marital Status	Other information as required	Other information as required such as the financial statement of the prospetive Customer or description on his/her principal consumers	
j.	The identity of Beneficial Owner if any			
k.	Occupation (name of a company/ institution, address of a company/ institution, and the official position)			
l.	Average incomes			
m	The purpose and intended nature of the business relationship			
n.	Other information that makes the Bank			

Natural Person		Legal Person (including Bank)	Charity/ Association	State/Government Institutions, international organization, foreign country representatives
	be able to identify the profiles of a prospetive Customer			

4. In the event a person who will engage a transaction with the Bank is WIC, information that must be requested by the Bank shall cover at least as follows:

Table 2: Information on WIC

WIC engaging a transaction in the amount of Rp 100,000,000.00 (one hundred million Rupiah) or more or in equivalent amount			WIC engaging a transaction less than Rp 100,000,000.00 (one hundred million Rupiah) or in equivalent amount	
Natural person		Legal Person	Natural person	Legal Person
a.	Full name including alias	Name of company	Full name including alias	Name of company
b.	Number of the identification document	A business license number issued by the competent authority	Number of the identification document	Domicile
c.	Address described in the identification document	Domicile	Address described in the identification document	
d.	Current address including phone number if any	Place and date of establishment		
e.	Place and date of birth	Type of legal entity		
f.	Nationality	The Identity of beneficial owner if any		
g.	Occupation	Sources of fund		
h.	Gender	The purpose and intended nature of		

WIC engaging a transaction in the amount of Rp 100,000,000.00 (one hundred million Rupiah) or more or in equivalent amount			WIC engaging a transaction less than Rp 100,000,000.00 (one hundred million Rupiah) or in equivalent amount	
Natural person		Legal Person	Natural person	Legal Person
		the business relationship		
i.	Marital Status	Other information as required		
j.	The Identity of Beneficial Owner if any			
k.	Sources of fund			
l.	Average income			
m	The purpose and intended nature of the business relationship			
n.	Other information that makes the Bank be able to identify the profiles of a prospetive Customer			

5. A transaction with WIC whose value is in the amount of Rp.100,000,000.00 (one hundred million rupiah) or more or in an equivalent amount conducted in 1 (one) time or multiple transactions within 1 (one) business day as referred to in Table 2 shall be a transaction that meets the following criteria:
   a. Is engaged at same Bank' office; and
   b. Types of transaction engaged are similar such as deposit, withdrawal, transfer, cash the cheques, and is not a compilation of various transactions whose types are different.

C. The Request of Documents

1. For natural person Customers, information described in Table 1 and Table 2 above must be supported with applicable identification documents attaching the Customer's picture and issued by the competent authority.

2. Main supporting documents on identity of natural person Customers who are Indonesian shall be Identity Card (*Kartu Tanda Penduduk* (KTP)), Driving License, or passport that are still applicable. Additional supporting document shall be Tax Register Number (*Nomor Pokok Wajib Pajak* (NPWP)).
3. For the prospective Customers who are foreign natural persons, identification documents shall be passport and stay permit based on regulations on immigration. If the prospective Customers are foreign country citizen and do not stay in Indonesia, stay permit documentation may be replaced with others that may provide assurance to the Bank on the profiles of the prospective Customer concerned such as a reference letter from an Indonesian citizen or a company that has been a Customer of the Bank, or a reference from Indonesian government institution/agency informing profiles of the prospective Customer concerned.
4. For the prospective Customers who are legal persons, the identification documents that may be requested as follows:
    a. Deed of establishment and/or article of association of a legal person. For a legal person who is foreign legal entity, the identification documents shall be other documents alike of deed of establishment and/or article of association based on prevailing laws and regulation issued by the competent authorities of a country where such legal person resides; and
    b. A business license or other license issued by the competent authority. For example, a business license from Bank Indonesia for Foreign Exchange Traders and Money Remittance Services, or a business license from the Ministry of Forestry for businesses in woods/forestry (Forest Concessions, Industrial Plants Forest, the Use of Timber Permit, General Work Plan, and Annual Work Plan).
5. For the prospective Customers like charity or associations, the identification documents that must be requested respectively the deed of establishment issued by the competent authority and/or a license on activity/objectives of the charity or a reference informing that they have been registerred as associations.
6. Besides the identification documents, the Bank shall oblige to obtain other documents as follows:

Table 3: Supporting Docments of the Prospetive Customers who are Natural Persons and Legal Persons

Natural Person		Legal Person (Non Bank)		Legal Person in a form of the Bank
		Micro Business and Small Enterprise	Non Micro Business and Small Enterprise	
a.	Signature Speciment	Signature Speciment of the Mangement or the party provided with the power of attorney to enter into a business relationship with the Bank	Signature Speciment of members of the Board of Directors authorized to represent a company or the party provided with the power of attorney to enter into a business relationship with the Bank	Signature Speciment of members the Board of Directors authorized to represent a company or the party provided with the power of attorney to enter into a business relationship with the Bank
b.		Tax Registration Number for the Customer required to have Tax Registration Number pursuant to prevailing laws and regulation	Tax Registration Number for the Customer required to have Tax Registration Number pursuant to prevailing laws and regulation	
c.		Business Location Permit (SITU) or other documents required by the competent authority	Business Location Permit (SITU) or other documents required by the competent authority	
d.			Financial staement or description on business activity of a company	
e.			Managerial Structure of a Company	

Natural Person		Legal Person (Non Bank)		Legal Person in a form of the Bank
		Micro Business and Small Enterprise	Non Micro Business and Small Enterprise	
f.			Ownership structure of a Company	
g.			The identificaiton document of members of the Board of Directors authorized to represent a Company or the party provided with the power of attorney to enter inti a business relationship with the Bank	

7. For the prospective Customers other than as mentioned in Table 3 above, the Bank shall oblige to obtain other documents besides the identification documents, which are:

Table 4: Supporting Documents for Non Natural Persons and Legal Persons

Charity		Association	State/Government Institution, International Organization, Foreign Country Representative
a.	Description on activities of the Charity	Name of the management	An appointment assignment for parties authorized to represent the agency or representative in entering into a business relationship with the Bank
b.	Managerial structure of the Charity	Party authorized to represent an association in entering into a business relationship with the Bank	Signature speciment

	Charity	Association	State/Government Institution, International Organization, Foreign Country Representative
c.	The identification document of the management authorized to represent a foundation in entering into a business relationship with the Bank		

D. Beneficial Owner

1. The Bank shall oblige to assure if the prospective Customer or WIC represents a Beneficial Owner in entering into a business relationship or engaging transactions with the Bank.
2. If the prospective Customer or WIC represents a Beneficial Owner in enterning into a business relationship or engaging transactions, the Bank shall oblige to perform CDD procedure against a Beneficial Owner as stringent as CDD procedure applied for the prospective Customer or WIC.
3. On a Beneficial Owner (BO), the Bank shall oblige to obtain evidence on identity and/or other information similar with the prospective Customer as mentioned in Table 1, Table 3, and Table 4, supported with the following:

Table 5: Evidence/other information related with beneficial owners

Beneficial owner of the natural person Customer		Beneficial owner of the legal person Customer /Charity /Association	Beneficial owner of the Customer like the Bank	
			Other domestic Bank	Other foreign exchange Bank*)
a.	Legal relationship between a Customer or WIC and the Beneficial Owner appointed upon an assignment statement, a contract, power of attorney or other type.	Documents and/or information on identity of the true owner or the owner of the controlling interest of a company, foundation or association	Written statement from domestic Bank that identity of the Beneficial Owner has been verified by other Other	Written statement from domestic Bank that identity of the Beneficial Owner has been verified by such

Beneficial owner of the natural person Customer		Beneficial owner of the legal person Customer /Charity /Association	Beneficial owner of the Customer like the Bank	
			Other domestic Bank	Other foreign exchange Bank*)
			domestic Bank Bank	foreign exchange Bank
b.	A statement from a prospetive Customer or WIC regarding accuracy of identity or sources of fund from the Beneficial Owner	A statement from a prospetive Customer or WIC regarding accuracy of identity or sources of fund from the Beneficial Owner		

*) Other bank abroad shall be other Bank located abroad tha applies AML and CFT Program equavalently with provisions issued by Bank Indonesia.

4. For legal person Customers, parties shall be the controllers if they meet the following requirements:
   a. Have shares of the company both directly or indirectly of 25% (twenty five persentage) or more from total shares issued and have a voting right; or
   b. Have shares of the company less than 25% (twenty five persentage) from total shares issued and have a voting right but persons concerned may be proved to have performed the Controlling against the company both directly or indirectly.

   The final controller shall be if the natural persons or legal persons have shares of the company both directly or indirectly and are final controllers of the company and/or entire group structure of the business that controls the company.
5. For natural person Customers who are the controllers shall be if they have the interest on a transaction engaged.
6. The identification document of the owner or final controller may be in form of a statement or other document containing information on identity of the owner or final controller.

7. If the Beneficial Owner is a government institution or company listed in the stock exchange (listing), the obligation for submitting documents and/or identity of final controller shall be exempted or inapplicable. In this case, this includes legal person Customers that are subsidiaries of a company listed in the stock exchange (listing) in which ownership of its principal company is majority.
8. If the Bank is doubt or may not assure on identity of the Beneficial Owner, the Bank shall oblige to refuse to enter into a business relationship or engage a transaction with the prospective Custoemer of WIC.
9. The Beneficial Owner subject with exemption must be documented.

E. Documents Verification

1. Information presented by the prospective Customer/Customer/WIC associated with its supporting documents must be examined those accuracy by performing verification process on such supporting documents based on other documents and/or information that may be realiable and independent and ensuring that such data is updating.
2. In ensuring the accuracy of identity of the prospective Customer, verification shall be performed thru:
    a. Face to face communication with the prospective Customer at beginning of a business relationship. In this case, the Bank may be represented by other party who understands basic principles of AML and CFT as well as CDD procedures implemented by the Bank. If face to face communication with the prospective Customer may not be performed at beginning of a business relationship with the Bank, the obligation for conducting face to face communication may be performed later insofar the Bank has met requirements at least as the following:
        1) The prospective Customer is classified as low risk;
        2) the certification of documents presented by the prospective Customer issued by the competent authority;
        3) Financial transactions with the Bank (such as payments or deposits) at first shall be conducted in cash at the Bank issuing a product owned by the Customer that resides within Indonesia; and

4) Conducting more stringent monitoring.

b. Conducting interview with the prospective Customer if required.

c. Verifyng the accuracy of profiles of the prospective Customer by checking his/her picture attached in the identiy card.

d. Requesting the prospective Customer for providing other identification document issued by the competent authority if there is an unlikelihood occured on the identiy card presented.

e. Keeping records on identification documents as from performing verification on legitimate original documents.

f. Conducting cross-examination to ensure consistency derived from various information submitted by the prospective Customer as the following:

1) Contacting the Customer by phone (home or office);

2) Contacting the officer of Human Resources Division where the Customer works if s/he is an employee of a company or institution;

3) Conducting a confirmation on incomes of the Customer by requiring to submit an account book from other Bank that resides within Indonesia; or

4) Conducting an analysis on geographical information system in order to seek forestry condition using remote sensing technology for the prospective Customers whose companies are in forestry sector.

Examination as mentioned above shall also include examination on names of the prospective Customer against:

1) Terrorists List.

2) National Black List (DHN) issued by Bank Indonesia.

3) Other lists possessed by the Bank (if any).

4) Others such as major credit card, identity of an employer of the prospective Customer, phone and electricity bills.

g. Ensuring possibility on unusual or suspicious matters.

3. Verification process on identity of the prospective Customer and Beneficial Owner must be completed prior entering into a business relationship with the

prospective Customer or before engaging a transaction with WIC.

4. In certain circumstances, verification process may be completed later, in which within no later than:
   a. 14 (fourteen) business days as from entering into a business relationship for natural person customers.
   b. 90 (ninty) business days as from entering into a business relationship for legal person customers.

   Certain circumstances as mentioned above shall be as follows:
   a. Completion of documents cannot be achieved when a business relationship will be performed due to such documents are still being processed; and
   b. If the prospective Customer is classified as low risk.

F. Simplified CDD

1. The Bank may apply simplified CDD procedures against the prospective Customers or transactions whose risk rate is low on potential money laundering and the financing of terrorism and shall meet criteria as follows:
   a. The purpose of the opening of an account is dealing with payroll. If this case, such account shall be an account owned by a company for reimburing salaries of employees of a company concerned or an account of the natural person whose purposes of the opening of an account is to collect salaries paid by his/her company periodically;
   b. The Customer is public company (company listed in the stock exchange house) that applies regulations concerning the obligation for disclosing its performance so that information on identification documents of such company as well as its beneficial owners may be accessed by public;
   c. The Customer is a Governent Agency; or
   d. A transaction for disbursing a check performed by a legal person WIC.
2. Information and documents required by the prospective Customer subject with simplified CDD shall be as follows:

Table 6: Simplified CDD

Natural Person		Legal Person (non Bank)		Corporate WIC
		Micro business and small enterprise	Non micro business and small enterprise	
a.	Full name as well as alias if any	Name	Name	Name
b.	Number of the Identification Document	Domicile	Domicile	Domicile
c.	Domicile described in the identification document	Signature speciment of members of the Board of Directors authorized to represent a company or the party who is provided with power of attorney in entering into a business relationship with the Bank	The identification document of members of the Board of Directors authorized to represent a company or the party who is provided with power of attorney in entering into a business relationship with the Bank	
d.	Current domicile including phone number if any			
e.	Place and date of birth			
f.	Identification document			

3. On the Customers subject with simplified CDD, the Bank shall oblige to keep their records into a list among others containing information on the rationale of risk determination that they are classified as low risk.
4. If the Customers subject with simplified CDD engage transactions that indicate the comission of money laundering or the financing of terrorism, then simplified CDD procedures shall be no longer applicable, but instead on the Customers concerned must be subject EDD and removed from simplified CDD list.

CHAPTER VI
HIGH RISK AREAS AND POLITICALLY EXPOSED PERSONS (PEP)

A. Criteria Determination on High Risk Area and PEP

In classifying a Customer based on its risk level, Banks may use PPATK regulation concerning on Guidelines on the Identification of High Risk Products, Customers, Business and Countries for Financial Service Providers (hereinafter referred to as PPATK's Identification Guidance).

High- risk area in this Guide is based on either to PPATK's Identification Guidance or to other references issued by legal authority or has become *International Best Practice.*

1. High Risk Product and Services

Characteristics of high-risk products and high-risk services are product/services offered to customers that easily converted into cash or equivalent with cash, or its fund is easily moved from one jurisdiction to other jurisdiction with the purpose to conceal the origins of such fund. For instance:

a. Electronic Banking;
b. Internet Banking;
c. Fund Transfer;
d. Facility of Credit and Leasing (including Credit Card)
e. Travelers' Cheque and Bank Draft;
f. Private Banking;
g. Custodian;
h. Safe Deposit Box;
i. Mutual fund;
j. Bank notes trading (Bank notes); or
k. Letter of Credit (LC).

2. High Risk Customer

State official or PEP is an example of high-risk customers. Law and regulation concerning on state officials are:

Table 7: Provisions on PEP

Provision	Definition	Description
Law Number 28 Yr 1999	State Officials who perform function of legislative, executive and judiciary and other officials performing function and duties in relation with the state administration based on prevailing laws and regulation.	• The State Official in the Highest State Institution; • The State Official in the High State Institution; • Ministers; • Governors; • Judges; • Other State Officials based on prevailing laws and regulations, and • Other Officials who have strategic function in relation with the state administration based on prevailing laws and regulations
SE/03/M.PAN/01 /2005 dated on 20 January 2005	State Officials	• An Official echelon II and other Official similar within government institutions or state agency; • All heads of offices within the Ministry of Finance; • Supervisors of Customs and Excise; • Auditors; • An Official issues licensing; • An Official/Head of Society Unit; and • An Official of regulators

3. High Risk Business

The following businesses are categorized as high-risk business:

a. Securities brokers who perform a function as securities intermediary (corporate customer);
b. Insurance company and insurance brokers (corporate customer);
c. Money Changer (corporate customer);
d. Pension Fund and financing business (corporate company);
e. Bank and company domiciled in countries producing drugs, NCCT or tax haven countries;
f. Casino, amusement places and executive club;
g. Money remittance services;
h. Accountants, lawyers and notary services (corporate/individual);
i. Surveyor services and real estate agents (Corporate);
j. Precious stone traders (Corporate/individual);
k. Antique shops, car dealer, ships and luxury goods trader;
l. Travel agents;
m. Employees of the Bank;
n. Students/college students; or
o. Housewife.

4. Transaction related with high risk countries

The following criteria are categorized as high-risk country:

a. countries which do not or insufficiently apply the FATF Recommendations;
b. Listed in the FATF *statement*;
c. Countries commonly known as places producing and central of drugs trafficking;
d. Countries commonly known to apply strict banking secrecy laws;
e. Commonly known as tax haven i.e the latest data from Organisation for Economic Cooperation and Development (OECD). As of May 2009 the following 35 countries/jurisdictions categorized as tax haven:

Aruba	Cook Islands	Malta	San Marino

Anguilla	Cyprus	Marshall Islands	Seychelles
Antigua and Barbuda	Dominica	Mauritius	St. Lucia
Bermuda	Gibraltar	Montserrat	St. Kitts & Nevis
Bahamas	Grenada	Niue	St. Vincent and the Grenadines
Bahrain	Guernsey	Nauru	Turks & Caicos Islands
Belize	Isle of Man	Netherlands Antilles	US Virgin Islands
British Virgin Islands	Jersey	Samoa	Vanuatu
	Liberia	Panama	Cayman Islands

f. countries that has high corruption;

g. countries considered sources of terrorist activity, such as identified in Office of Foreign Asset Control (OFAC); or

h. Countries imposed with the UN sanctions.

In relation with high risk area above, Banks are required to scrutinize the existence of Customers and Beneficial Owners that met the high risk criteria and document them in a separate list.

B. Procedure to High Risk Area and PEP

1. If there is a transaction or business relationship with a Customer originating or associated with countries that have not implemented FATF recommendations adequately, Banks are required to be vigilant and determine risk mitigation may arise.
2. In the event, Banks intend to enter into a business relationship with prospective Customers classified as high risk (in this case is PEP), Banks are required to appoint a senior management duly responsible for the business relationship with such Customers and shall be authorized to:

a. approve or refuse a prospective Customers classified as high risk or PEP; and
b. Decide to continue or terminate business relationship with Customers or Beneficial Owners classified as high risk or PEP.

3. A senior management shall possess adequate knowledge of arising risk for instance reputation risk, operational risk, and legal risk and shall possess the ability to make necessary decisions according to the risk profile of the Customer and transaction.

C. Enhanced Due Diligence (EDD)

1. EDD or a comprehensive CDD activity shall be conducted to high-risk area and Customer categorized as PEP.
2. Nature, quality, and quantity of Customer on information obtained shall provide a picture of risk level may arise from the occurring business relationship.
3. Finding information shall be verified and may convince the Bank on a real customer's profiles.

CHAPTER VII
CDD IMPLEMENTATION PROSCEDUR PERFORMED BY THIRD PARTY

A. Criteria of Third Party and Procedures

1. The Bank may use the result of CDD that has been performed by the third party on prospective Customers who have been Customers of the third party concerned already. In this case, the Bank remains requiring to perform identification and verification on the result of CDD conducted by the third party.
2. The third party as mentioned in point 1 shall be financial institutions based on prevailing laws and regulations.
3. The third party of non financial institutions that performs CDD upon a contract (outsourcings or agents) is not classified as the third party as governed in this provision by considering that outsourcings or agents are intemediaries of the Bank concerned, not as the third party.
4. The result of CDD that may be used by the Bank shall be the result from third party that meet at least the following creteria:
    a. To have CDD procedure based on prevailing laws and regulations;
    b. To have cooperation with the Bank upon a written agreement;
    c. Shall be a financial institution subject to supervision by the competent authority (such as Bank Indonesia or Bapepam-LK) based on prevailing laws and regulations;
    d. Is willing to meet a request of information whereby at least shall be information on:
        1) Full name as mentioned in the identification document;
        2) Address, place and date of birth;
        3) Identify card number; and
        4) Nationality of a prospective Customer,

and copies of the supporting documents as required by the Bank in order to implement AML and CFT Program. Such willingness shall be described into a written agreement as mentioned in letter b; and

e. Status of a Country that has applied FATF Recommendations. Information on compliance of FATF Recommendations of a country may be seen in Mutual Evaluation Report that can be accessed from website www.fatf-gafi.org or www.apgml.org).

5. Final responsibility on the result of identification and verification against a prospective Customer shall be completely under the Bank.
6. The Bank shall be responsible to implement record-keeping on the result of CDD performed by the third party as well as data on results of identification and verification performed by the Bank.

B. The Bank as a Broker

1. If the Bank is acting as the selling agent of products of other financial institution (such as mutual funds), the Bank acting as the selling agent shall oblige to meet a request of information on the result of CDD and copies of supporting documents if required by other financial institution (for example the Investment Manager) in implementing AML and CFT Program.
2. Such obligations of the Bank shall be prepared in cooperation between non-Bank financial institution and the Bank into a written agreement pertaining a willingness of the Bank to provide information as referred to in letter A point 4.d.

CHAPTER VIII
CROSS BORDER CORRESPONDENT BANKING

A. Cross Border Correspondent Banking Procedure

1. Prior to providing Cross-border Correspondent Banking services, Banks shall conduct CDD process to respondent Bank either acting as Beneficiary Banks or as Intermediary Banks. Beneficiary Banks or Intermediary Banks in L/C transaction shall include issuing bank, advising bank, confirming bank, and negotiating Bank.
2. CDD process conducting by request information concerning:
   a. Profiles of prospective beneficiary Banks and/or Intermediary Banks that include the compositions of the Board of Directors and the Board of Commissioners, business activities, banking product, marketing target, and purpose of opening account. Information sources for ensuring the validity information shall be based on adequate public information issued and established by authority i.e. Banker's Almanac;
   b. reputations of Beneficiary Banks and/or Intermediary Banks based on information that is accountable, including negative reputation such as sanctions that have been imposed by the authority against such Banks and/or Intermediary Banks, in relation with violation of provisions issued by the authorities and/or FATF Recommendations;
   c. level of compliance of APU and PPT Program in a country where the Beneficiary Banks and/or Intermediary Banks domicile; and
   d. other relevant information required by Banks in identifying the profile of prospective Beneficiary Banks and/or Intermediary Banks i.e. Ownership, controlling and structure of management, to ascertain the existence of PEP within the ownership structure or as controllers, financial position of the Beneficiary Bank and/or Intermediary Bank, and profiles of the principal/holding company and subsidiaries.
3. Ordering Banks providing Cross Border Correspondent Banking services shall be required to:

a. document all Cross Border Correspondent Banking transactions;
b. refuse to have dealings and/or continue dealings of Cross Border Correspondent Banking with shell Banks; and
c. Ensure that Recipient Banks and/or Intermediary Banks do not permit their accounts to be used by Shell Banks when engaging business dealings associated with Cross Border Correspondent Banking.

4. Approval for both opening new correspondent relationships and terminating business relationship with existing Cross Border Correspondent Banking obtained by senior management.

B. Payable Through Account

1. For Customers that have access to Payable Through Accounts (PTA), Ordering Banks shall ensure,:
   a. Beneficiary Banks and/or Intermediary Banks has performed adequate CDD and monitoring processes, at least equivalent to standards stipulated in the Bank Indonesia Regulation; and
   b. Beneficiary Banks and/or Intermediary Banks are able to provide relevant Customer identification data upon request to the Transferring Bank.
2. Access to PTA that oblige be ensured by Ordering Bank shall be conveyed in cooperation between Ordering Bank and Beneficiary Banks and/or Intermediary Banks in the form of a written agreement.
3. The example of PTA transaction:

   Bank A (established and under supervisory of South Pacific Island Vanuatu authority) opened PTA at American Express Bank International (AMEX) at Miami, US. The purpose of opening PTA is to make Bank A in Vanuatu able to offer AMEX banking services virtually to his American Customers who reside in Vanuatu jurisdiction but they are not the holder of AMEX account.

   The Customer will have chequebook including the application that either give them access to do deposit or withdrawal through Bank A's PTA. This PTA transaction might be misuse of either account or transaction, and pose reputation risk for AMEX.

CHAPTER IX
WIRE TRANSFER PROCEDURE

A. Wire Transfer Procedure

1. In performing wire transfer activities, Ordering Banks shall require to obtain information and perform identification as well as verification on the Originator, which shall at least cover:

Table 8: Wire transfer Information

	Domestic Wire Transfer *)	International Wire Transfer
a.	The Name of the originator	The Name of the originator
b.	the originator's account/identity number	the originator's account/identity number
c.	Date of transaction, effective dates, currency types, and nominal	Date of transaction, effective dates, currency types, and nominal
d.		Addresses or place and date of birth

*) The provisions shall also apply to the wire transfer through the use of cards such as debit cards, credit cards, and ATM card.

2. Banks should be required to maintain all wire transfer records on transactions.
3. In the event, the Originator not complying with information request referred to Table 8, by using a risk based approach, Ordering Banks may:
   a. refuse to do wire transfer;
   b. cancel wire transfer transaction; and/or
   c. Terminate business relationship with existing customers.
4. Intermediary Banks shall forward messages and or wire transfer instructions, as well as administer information received from Ordering Banks.
5. For domestic wire transfer, Beneficiary Banks shall ensure completeness of information of the originator.

B. Information Request

1. If needed, Intermediary Banks and Beneficiary Banks may ask information relating to the originator of the wire transfer as referred to in Table 8 to Ordering Bank.
2. Information request shall be made in writing from the competent officer through either by letter or by electronic media.
3. Relating to domestic wire transfer, Ordering Banks shall submit written information to Intermediary Banks and/or a recipient Banks within 3 (three) business days of receiving a request.
4. The exchange of information between/among banks as referred to in number 1 is confidential and only can be used for the purpose of transaction analysis, investigation, and competent authority need.
5. Providing information request from Intermediary Banks or Beneficiary Banks conducted for the purpose of exchange of information between/among Banks, so that it exempted from bank secrecy provisions. The request and submitting information shall be documented.

C. Reporting

If there is a wire transfer in both the form of incoming or outgoing, domestic or international, and meets the suspicious criteria, Banks shall be required to report the wire transfer as Suspicious Financial Transactions to PPATK**.** In this matter, including to transaction suspected to be associated with terrorism or financing of terrorism.

CHAPTER X
INTERNAL CONTROL SYSTEM

1. The Bank is required to institute segregation of operational function and oversight function.
2. The application of AML and CFT Program requires separation of duties and responsibilities between:
   a. those implementing policies and those supervising on policies implementation, and
   b. those implementing transactions and those making decisions on transaction.
3. Banks must have a proper internal control system, both functionlal and built-in, capable of ensuring that application of AML and CFT Program by relevant units complies with established policies and procedures.
4. The internal audit unit (SKAI) as a unit assigned to implement internal control has authority and sufficient facilitation shall at minimum include:
   1) the program and risk based audit procedur encompassing compliance test which focus on CDD, operational, high risk product and high risk service;
   2) the assesment of adequacy of prevailing proces in a Bank while doing identification and reporting unusual transaction;
   3) timely reporting of examination finding to Board of Directors and/or management; and
   4) the recommendation of rectifying action with respect to occured f inding.
5. Internal control system must be capable of timely detection of weaknesses and irregularities that may arise in implementing AML and CFT Program with the objective of minimizing the risk exposure of the Bank.

CHAPTER XI
INFORMATION MANAGEMENT SYSTEM

A. Information Management System

1. For the purpose of monitoring the profiles of Customer's transactions, the Bank shall oblige to possess information system that be able to identify, analyze, monitor or provide reports effectively on characteristics of such transactions engaged by the Bank's Customers.
2. Information system possessed must be able to make the Bank possibly traces any individual transaction both for internal interest and or for the interest of Bank Indonesia, as well as in relation with the court cases.
3. Level of sophistication of information system in identifying suspicious financial transactions shall be adjusted with complexity of transactions, volume of transactions and risks possesed by the Bank.
4. The Bank shall oblige to conduct parameter adjustment periodically that is used for identifying suspicious financial transactions.
5. For facilitating monitoring in order to analyze suspicious financial transactions, the Bank shall oblige to have and maintain Single Customer Identification File (CIF), in which at least including information as referred to in Table 1 attached in Chapter V.
6. Information included in single CIF shall contain all accounts maintained by Customers at a Bank such as saving accounts, certificate of deposits, giro and loans.
7. On a joint account, there two approaches as the following:
   a. If the owners of a joint account (Accounts A and B) have also other accounts under their own name (Account A and Account B), CIF prepared shall be 2 (two) CIFs which are CIF under name of A and CIF under name of B. Each CIF must inform that both A and B have a joint account.

b. If the owners of a joint account (Accounts A and B) no longer have other accounts, then CIF prepared shall cover information on A and B.

8. For the purpose of maintenance of single CIF, the Bank shall oblige to determine policies that if there is any additional account opened by an existing Customer, the Bank has to relate such additional account to Customer Identification File of a Customer concerned.
9. In the event that there is a Customer either registered as a Customer of the conventional Bank or the Islamic Bank similarly, a Customer concerned shall have two different CIFs.

B. Monitoring

1. The Bank shall oblige to conduct monitoring at least including issues as the following:
   a. Monitoring is performed continuingly for identifying accuracy between the Customer's transactions and profiles and keeping such records, in particular on business relationship/transactions with the Customer and/or the Bank from a country that applies AML and CFT unsufficiently.
   b. Conducting an analysis against all tranasctions that are unfitting with the Customers' profiles. For example, transactions, activities, and behavior that are unfitting with the Customers' profiles as attached in Appendix III.
   c. If required, requesting for information on the background and purposes of transactions against transactions unfitting with the Customers' profiles by considering provisions on anti tipping-off as stipualted in Law concerning Money Laundering Crime.
2. Monitoring activity on the Customers' transactions and profiles undertaken continuingly shall include as the following:
   a. Assuring completeness of information and documents of the Customers;
   b. Examining accuracy between the Customers' profiles and the Customers' transactions profiles.
   c. Examining likeness or similarity of names with names included in the terrorist list database; and

d. Examining names' likeness or similarity with names of suspects or defendants published in mass media or issued by the competent authorities.

3. Sources of information that may be used for monitoring the Bank's Customers determined as a suspect or defendant that may be obtained thru:
   a. Databases issued by the competent authority such as PPATK; or
   b. Mass media such as newspapers and magazines.
4. Monitoring on the Customers' profiles and transactions must be conducted periodically using risk based approach.
5. If there is likeness or similarity of names as mentioned in point 2 letters c and d above, the Bank shall oblige to conduct clarification in order to assure such likeness.
6. In the event the Customer's name and identification document is suitable with names of suspects or defendants informed in mass media and/or based on terrorists list as mentioned in point 2 letters c and d, the Bank shall oblige to report the Customer concerned in a Suspicious Financial Transaction Report.
7. Monitoring on the Customers' accounts must be observed strictly if there are:
   a. Transaction of money remittance related with the Customers residing in high risk countries;
   b. Credit card that has been over payment whose values are significant;
   c. A debtor who is a foreign legal person using guarantee like back to back LC and/or standby L/C.
8. All monitoring activities shall be documented orderly.

C. Terrorists List Database

1. The Bank shall oblige to maintain terrorists list obtained from Bank Indonesia every 6 (six) month based on data published by the United Nations.
2. Information on terrorists list may be obtained from the following:
   a. The United Nations' website: http://www.un.org/sc/committees/1267/consolist.shtml ;

b. Other source that is commonly used by banking and shall be public information such as the Office of Foreign Assets Controls List (OFAC List) in which this can be accessed from: http://www.treas.gov/offices/enforcement/ofac/index.shtml ; or

c. The competent authorities such as information from PPATK or the Police, so that the Bank may actively update Terrorists List disregarding waiting for the list sent by Bank Indonesia.

3. Monitoring activity that must be conducted by the Bank in relation with terrorist list database possessed shall be:

a. Assuring periodically if there are names of the Bank's Customers that have similarity or likeness with names incouded in such database.

b. If there is likeness between name of the Customer and names described in Terrorists List database, the Bank shall oblige to assure the accuracy of identification document of the Customer concerned with other relevant information.

c. If there is similarity between name of the Customer and other information with names described in Terrorists List database, the Bank shall oblige to report the Customer concerned in a Suspicious Financial Transaction Report.

D. Data Updating as a Following Up of Monitoring

1. The Bank shall oblige to conduct data updating on information and documents as referred to in Articles 13, 14, 15, 16, 17, 18 and 19 of Bank Indonesia Regulation Number 11/28/PBI/2009 concerning Anti Money Laundering and Combating the Financing of Terrorism Program and its Record Keeping.
2. The Bank shall oblige to conduct data updating on its Customers that identification and monitoring of suspicious financial transactions can be implemented effectively.
3. Customers' data updating shall be conducted by using risk based approach including updating the Customers' profiles and their transactions. If existing human resources of the Bak are limited, data updating shall be implemented using priority scale.

4. Parameters used in determining priority scale as referred to in point 2 shall be as the following :
   a. The customer's risk rate is high;
   b. Transaction is engaged in significant amount of money and/or deviated from transactions' profiles or the Customer' profiles (red flag);
   c. The balancing is in significant amount of money; or
   d. Existing information included in CIF has not been complied with requirements as governed in Bank Indonesia Regulation concerning AML and CFT.
5. Data updating shall be performed periodically on the ground of the Customers/transactions' risk rate. For example, data updating for high risk Customers shall be conducted every 6 months, data updating for low risk Customers shall be conducted every 2 years, and data updating for medium risk Customers shall be conducted annually.
6. Implementation of data updating may be conducted when:
   a. Opening an additional account;
   b. Renewing loan facility; or
   c. Replacing books of saving accounts, ATM or other banking product documentation.
7. Registration of updated Customers' information into CIF without supported with documents must be subject an approval from the authorized Bank's Official.
8. All data updating activities must be recorded.
9. In performing such data updating, the Bank shall oblige to conduct monitoring on the Customers' information and documents.

E. Termination of a business relationship with an existing customer

1. The Bank may terminate a business relationship with the Existing Customer if:
   a. The Existing Customer concerned does not comply with requirements on request for information and supporting documents as referred to in Table 1, Table, 3, and Table 4;
   b. The Bank is doubtful on accuracy of the Customer's information; or

c. Utilization of an account is inconsistent with the Customer's profiles.

2. If the Bank remains maintaining a business relationship with the Existing Customer as referred to in point 1 (one) above, the Bank at least shall oblige to:
   a. Have reasonable grounds to maintain a business relationship, and
   b. Report the Customer concerned in an STR.

F. Suspicious Financial Transaction Reports Resulted from Monitoring

Upon the result of monitoring on the Customer's profiles and transactions, the Bank shall oblige to report as an STR if:

1. The Customer does not compley with requirements as referred to in letter B point 6;
2. The Customer whose business relationship is closed down due to unavailability of information and supporting documents and based on the Bank's evaluation that a transaction engaged is unusual or suspicious;
3. The Customer/WIC whose transaction is refused or cancelled due to unavailability of information and supporting documents and based on the Bank's evaluation that a transaction engaged is unusual or suspicious; or
4. A transaction that meets criteria of suspicious as referred to in Law concerning Money Laundering Crime.

CHAPTER XII
HUMAN RESOURCES AND EMPLOYEES TRAINING

A. Human Resources

1. The Bank shall oblige to perform the screening procedure when hiring employees as part of implementation of Know Your Employee (KYE).
2. Methodology of the screening procedure is modified with the needs, complexity of the Bank's activities as well as risks' profiles of the Bank.
3. Methodology of the screening procedure shall at least assure profiles of candidates that they do not have historical criminal records.
4. Conducting monitoring on profiles of employees.

B. Training

1. Training Participants

a. All employees must have knowledge on policies, procedures and implementation of AML and CFT Program.

b. Employees who have met criteria as the following:
   1) Interact in person with Customers (Customers' services);
   2) Perform daily duty related with supervision over implementation of AML and CFT Program; or
   3) Perform daily duty related with reporting obligation to PPATK and Bank Indonesia,

   shall get priorities to participate in training.

c. Employees who get priorities must participate in training periodically, and other employees who do not meet criteria mentioned in letter b above must get training program minimum 1 (one) time during their term of service.

d. Employees who enteract with Customers in person (front liner) must get training prior their placement.

2. Training Methodology

a. Training may be conducted both online based and discussions.
b. Online based training may be performed using *e-learning* media either provided by the competent authorities such as PPATK or independently by the Bank.
c. Face to face training shall be performed using the following approaches:
    1) Interactive discussions (for example workshops) whose topics of discussion are modified with participants' demand. This approach is used for employees who get priorities and organized periodically such as annually.
    2) One direction discussions (for example seminar) whose topics of discussion shall include general overview on implementation of AML AND CFT Program. This approach is provided to employees who do not get priorities and organized if provisions are amended significantly.

3. Topics and Evaluation of Training

a. Topics of training shall at least include:
    1) Implementation of laws and regulation in relation with AML AND CFT Program;
    2) Techniques, methodoloty and tipology of money laundering and the financing of terrorism including trends and development of risks' profiles of banking products; and
    3) Policies and procedures on implementation of AML AND CFT Program and roles and authority of employees in eradicating money laundering and the financing of terrorism, including consequences if employees conducting tipping off.
b. The Bank shall oblige to conduct evaluation on any training organized in order to identify level of understanding of participants and suitability of substances provided.
c. Evaluation may be conducted directly thru interviews or indirectly thru examination.
d. The Bank shall oblige to follow up results of evaluation obtained by improving training materials and methodology.

CHAPTER XIII
POLICIES AND PROCEDURES ON IMPLEMENTATION OF AML AND CFT AT THE BANK'S OFFICE AND SUBSIDIARIES IN FOREIGN JURISDICTION

A. The Bank's Office Located at Foreign Countries

1. The Bank that is an Indonesian legal entity shall oblige to carry on policies and procedures on AML and CFT Program to all offices located in foreign countries as well as to monitor its implementation.
2. If the Country of domicile of the branches has more stringent regulations on AML and CFT Program than regulations applied in Indonesia, such branches shall oblige to apply regulations issued by the competent authorities of such Country.
3. If the Country of domicile of the branches are based has not applied the FATF Recommendations or has applied the FATF Recommendations but its AML and CFT Program's standards are less strict than regulations applied in Indonesia, the branches shall be oblgied to apply AML and CFT Program as governed in Bank Indonesia Regulation.
4. In the event that regulations concerning implementation of AML and CFT Program applied in Indonesia create violatons against prevailing laws and regulations of the Country of domicile of the branches, the Bank's management located at such Country shall oblige to inform Head Office of the Bank as well as Bank Indonesia that such Bank cannot apply AML and CFT Program applicable in Indonesia.
5. Determination whether regulations of the Country of domicile of the branches are stringent or not must be supported with an analysis of each regulation applied.
6. For the purpose of monitoring implementation of AML and CFT Program in Branches located abroad, the Bank' office located at abroad concerned must

submit a report periodically to Head Office of the Bank on implementation of AML aned CFT Program in jurisdiction where the office resides.

B. Subsidiaries Located at Foreign Countries

1. The Bank that is an Indonesian legal entity shall oblige to carry on policies and procedures on AML and CFT Program to all subsidiaries located abroad as well as to monitor its implementation.
2. If the Country of domicile of the subsidiaries has more stringent regulations on AML and CFT Program than regulations applied in Indonesia, such subsidiaries shall oblige to apply regulations issued by the competent authorities of such Country.
3. If the Country of domicile of the subsidiaries has not applied the FATF Recommendations or has applied the FATF Recommendations but its AML and CFT Program's standards are less strict than regulations applied in Indonesia, subsidiaries shall be oblgied to apply AML and CFT Program as governed in Bank Indonesia Regulation.
4. In the event that regulations concerning implementation of AML and CFT Program applied in Indonesia create violatons against prevailing laws and regulations of the Country of domicile of the subsidiaries, the management of a subsidiary of the Bank located at such Country shall oblige to inform Head Office of the Bank as well as Bank Indonesia that a subsidiary cannot apply AML and CFT Program applicable in Indonesia.
5. Determination whether regulations of the Country of domicile of the branches are stringent or not must be supported with an analysis of each regulation applied.
6. For the purpose of monitoring implementation of AML and CFT Program in subsidiaries located abroad, subsidiaries concerned must submit a report periodically to Head Office of the Bank on implementation of AML and CFT Program in jurisdiction where subsidiaries reside.
7. Implementation of AML and CFT Program reported shall include statistical information on reporting in relation with AML and CFT Program.

CHAPTER XIV
RECORD KEEPING AND REPORTING

A. Record Keeping

1. The Bank shall oblige to keep records or documents properly in order to assist the competent authorities in performing investigation on funds being indicated to be derived from proceeds of crime or in implementing their duty. Accordingly, documents possessed/maintainted by the Bank must be accurate and complete so that its tracing is easy if required.
2. Time period of records keeping shall be as the following:
   a. Documents related with the Customer's data or Walk In Customer' data shall be maintained within no less than 5 (five years) as from:
      1) The terminatioan of a business relationship with a Customer or
      2) A Transaction engaged by WIC; or
      3) A transaction that has not apparent economic and/or visible lawful purpose is found.
   b. Documents of the Customer or WIC, which are related with a financial transaction within a period of time as referred to in Law concerning Corporate Documents.
3. Records that should be kept shall cover at least as the following:
   a. Identity of the Customer or WIC; and
   b. Information on a transaction including types of transactions and the amount of money engaged, date of a transaction, the origin and purposes of a transaction as well as the accounts' number related with a transaction.

B. Reporting

1. Reporting to Bank Indonesia

a. An Action Plan of Implementation of AML and CFT

1) An Action Plan shall be submited into a Report on Implementation of Duties of the Compliance Director of December 2009.
2) An Action Plan Report shall at least contain of stages in implementing AML and CFT Program in order to comply with Bank Indonesia Regulation concerning AML and CFT that must be enforced by the Bank based on a time period determined in An Action Plan, such as:
   i. Development of guidelines on AML and CFT;
   ii. Classification of Customers on the ground of Risk Based Approach;
   iii. Improvemnt of infrastructures in relation with information technology;
   iv. Preparation in developing Single Customer Identification File (CIF);
   v. Appointment of an employee who performs functions of a Special Unit at any branch office;
   vi. Availability of sufficient human resources;
   vii. Adjustment of information technology in implementing Customers' data updating program.
3) An Action Plan must obtain an approval from 2 (two) members of the Board of Directors who are the President Director and the Compliance Director.
4) Modification of an Action Plan may be conducted insofar changes are occurred out of the Bank's control and such modification shall be reported to Bank Indonesia.

b. Data Updating Plan Report

1) The Report shall be submitted annually into a Report on Implementation of Duties of the Compliance Director of second semester, in which for the first time shall be included into a Report of December 2010.
2) The Report must obtain an approval from 2 (two) members of the Board of Directors who are the President Director and the Compliance Director.

3) The Report shall refer to formats as attached in Appendix I.

c. Data Updating Realization Report

1) The Report shall be submitted into a Report on Implementation of Duties of the Compliance Director of second semester, in which for the first time shall be included into a Report of December 2011.
2) The Report submitted must obtain an approval from the Compliance Director.
3) The Report shall refer to formats of reporting as attached in Appendix II.

2. Reporting to PPATK

a. Submission of a suspicious financial transaction report and cash transaction report shall refer to provisions issued by PPATK.
b. Submission of a suspicious financial transaction report shall include a transaction suspected being related with terrorists' activity or the financing of terrorism.